DIGITELTS
by MADISON

Servicios de Emisión de Certificados Electrónicos

Declaración de Divulgación de PKI (PDS) para Certificados Cualificados

CONTROL DOCUMENTAL

NOMBRE	Declaración de Divulgación de PKI (PDS) para Certificados Cualificados de los Servicios de Emisión de Certificados Electrónicos de DIGITEL TS		
Distribución	**Público**		
Versión	V1.0		
Fecha	21/05/2026		
Aprobado	Comité de Riesgos y Seguridad de DIGITEL TS	Fecha	22/05/2026
Estado	Aprobado		

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
V1.0	21/05/2026	Primera versión del documento aplicable a todos los tipos de certificados cualificados emitidos por DIGITEL TS

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

Este documento constituye la Declaración de Divulgación de PKI (en adelante, "PKI Disclosure Statement" o PDS) del prestador de servicios de confianza cualificado DIGITEL TS para todos los tipos de certificados cualificados emitidos por su Autoridad de Certificación.

La presente PDS se ha elaborado de conformidad con el modelo de PKI Disclosure Statement definido en el Anexo A de la norma ETSI EN 319 411-1, y tiene como finalidad proporcionar a los suscriptores, firmantes, creadores de sellos y partes que confían en los certificados, una información clara, simplificada y accesible sobre los servicios de emisión de certificados cualificados prestados por DIGITEL TS, complementaria a la Declaración de Prácticas y Políticas de Certificación (DPPC). Esta PDS no pretende sustituir a la DPPC ni a las políticas de certificación contenidas en la misma.

DIGITEL TS presta sus servicios de emisión de certificados cualificados conforme a lo establecido en el Reglamento (UE) 910/2014 , relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, en lo que respecta al establecimiento del marco europeo de identidad digital (en adelante, "Reglamento eIDAS").

En adición, DIGITEL TS en la prestación de los servicios de emisión de certificados cualificados cumple con lo establecido en la normativa siguiente:

- Reglamento de Ejecución (UE) 2025/1943 de la Comisión, de 29 de septiembre de 2025, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a las normas de referencia para los certificados cualificados de firma electrónica y los certificados cualificados de sello electrónico
- Reglamento de Ejecución (UE) 2025/2530 de la Comisión, de 16 de diciembre de 2025, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los requisitos para los prestadores cualificados de servicios de confianza que prestan servicios de confianza cualificados.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Para los certificados cualificados emitidos a representantes de personas jurídicas y de entidades sin personalidad jurídica, así como al personal y a las organizaciones de las Administraciones Públicas españolas (Administraciones, organismos o entidades de derecho público), DIGITEL TS tiene en cuenta también lo estipulado en el documento titulado "Perfiles de certificados electrónicos 2.0" de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas en el marco de las Leyes españolas 39/2015 y 40/2015 y el Real Decreto 203/2021.

Para la identificación remota por video de solicitantes de certificados cualificados de firma y sello electrónicos amparados en la DPPC, se han tomado en consideración los requisitos definidos en la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados, modificada por la Orden ETD/743/2022, de 26 de julio.

Para garantizar la ciberseguridad y la ciberresiliencia de los servicios amparados en este PDS, Digitel TS ha alineado sus operaciones a los requisitos de seguridad de redes y de la información establecidos en la Directiva (UE) 2022/2555 (Directiva NIS2) y su Reglamento de Ejecución (UE) 2024/2690; así como, a la normativa de desarrollo que se dicte incluida la normativa de transposición al ordenamiento jurídico español.

Los certificados cualificados emitidos por DIGITEL TS son certificados emitidos al público.

Esta PDS se encuentra disponible en formato PDF/A conforme a la norma ISO 19005, y puede ser consultada en la dirección: https://pki.digitelts.es

2. INFORMACIÓN DE CONTACTO

- Razón Social: DIGITEL ON TRUSTED SERVICES S.L.U.
- Denominación Comercial: Autoridad de Certificación de DIGITEL TS
- NIF: B47447560
- Dirección. C/ Enrique Cubero 9, Edificio Madison Arena - 47014 Valladolid (España)
- Teléfono. +34 91 015 05 10
- Web: https://www.digitelts.es
- Email. info@digitelts.com
- Solicitud de revocación: La solicitud de revocación del certificado electrónico puede llevarse a cabo a través de la dirección de correo electrónico info@digitelts.com o de la Autoridad de Registro que emitió el certificado en cuestión, siguiendo el proceso descrito en la Declaración de Prácticas y Políticas de Certificación (DPPC).
- Registro Mercantil de Valladolid: Tomo 891, Folio 38, Sección 8, Hoja VA-11307

3. TIPOS Y FINALIDADES DE LOS CERTIFICADOS

DIGITEL TS ha asignado el OID 1.3.6.1.4.1.54225.10 para sus servicios de confianza de emisión de certificados electrónicos.

Los certificados de entidad final emitidos por la Autoridad de Certificación de DIGITEL TS incluirán los OIDs de políticas estándar para certificados cualificados de la Unión Europea emitidos para personas físicas y personas jurídicas conforme a lo establecido en ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-2 y 3, cuando resulten aplicables:

- Certificados cualificados de firma electrónica avanzada conforme a la política QCP-n definida en el estándar ETSI EN 319 411-2.
- Certificados cualificados de firma electrónica cualificada conforme a la política QCP-n-qscd definida en el estándar ETSI EN 319 411-2.
- Certificados cualificados de sello electrónico avanzado conforme a la política QCP-l definidas en el estándar ETSI EN 319 411-2.
- Certificados cualificados de sello electrónico cualificado conforme a la política QCP-l –qscd definidas en el estándar ETSI EN 319 411-2.

En adición, DIGITEL TS ha definido OID propios para identificar la política aplicable para cada perfil de certificado amparado en la DPPC.

Para los certificados que se expiden a representantes de personas jurídicas y de entidades sin personalidad jurídica, así como al personal y a las organizaciones de la administración pública española (Administraciones, organismos o entidades de derecho público), DIGITEL TS ha tenido en cuenta además los OID establecidos en el documento titulado “Perfiles de certificados electrónicos 2.0” de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas en el marco de las Leyes españolas 39/2015 y 40/2015 y el Real Decreto 203/2021.

A continuación, se describen los tipos de certificados cualificados emitidos por DIGITEL TS, sus identificadores de objeto propios de DIGITEL TS (OID), la política ETSI aplicable y, en su caso, el OID del perfil de certificado del Ministerio de Hacienda y Administraciones Públicas, los procedimientos de validación y las restricciones de uso de cada uno de ellos.

3.1 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA CUALIFICADA PARA CIUDADANOS [CENTRALIZADO]

OID de DIGITEL TS: OID 1.3.6.1.4.1.54225.10.3.5. Política ETSI: QCP-n-qscd (OID: 0.4.0.194112.1.2).

Estos certificados son certificados cualificados de firma electrónica de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo cualificado de creación de firma electrónica (QSCD), de acuerdo con el Anexo II del Reglamento (UE) 910/2014.

Estos certificados son gestionados de forma centralizada, es decir, la generación y gestión de los datos de creación de firma electrónica es realizada por el prestador, por cuenta del firmante.

Estos certificados garantizan la identidad del firmante, y permiten la generación de la "firma electrónica cualificada", con efecto jurídico equivalente al de una firma manuscrita conforme al artículo 25.2 del Reglamento (UE) 910/2014.

3.2 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA AVANZADA PARA CIUDADANOS [SOFTWARE]

OID de DIGITEL TS: OID 1.3.6.1.4.1.54225.10.3.1. Política ETSI: QCP-n (OID: 0.4.0.194112.1.0).

Estos certificados son certificados cualificados de firma electrónica de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados no funcionan con dispositivo cualificado de creación de firma electrónica (QSCD).

Estos certificados son gestionados de forma distribuida sin la participación de una herramienta de gestión centralizada.

Estos certificados garantizan la identidad del firmante, y permiten la generación de la "firma electrónica avanzada" basada en certificado cualificado de firma electrónica.

3.3 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA CUALIFICADA PARA PERSONAS FÍSICAS VINCULADAS [CENTRALIZADO]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.3.15. Política ETSI: QCP-n-qscd (OID: 0.4.0.194112.1.2).

Estos certificados son certificados cualificados de firma electrónica de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo cualificado de creación de firma electrónica (QSCD), de acuerdo con el Anexo II del Reglamento (UE) 910/2014.

Estos certificados son gestionados de forma centralizada, es decir, la generación y gestión de los datos de creación de firma electrónica es realizada por el prestador, por cuenta del firmante.

Estos certificados garantizan la identidad del firmante y su vinculación con la organización suscriptora del certificado, y permiten la generación de la "firma electrónica cualificada", con efecto jurídico equivalente al de una firma manuscrita conforme al artículo 25.2 del Reglamento (UE) 910/2014.

3.4 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA AVANZADA PARA PERSONAS FÍSICAS VINCULADAS [SOFTWARE]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.3.11. Política ETSI: QCP-n (OID: 0.4.0.194112.1.0).

Estos certificados son certificados cualificados de firma electrónica de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados no funcionan con dispositivo cualificado de creación de firma electrónica (QSCD).

Estos certificados son gestionados de forma distribuida sin la participación de una herramienta de gestión centralizada.

Estos certificados garantizan la identidad del firmante y su vinculación con la organización suscriptora del certificado, y permiten la generación de la "firma electrónica avanzada" basada en certificado cualificado de firma electrónica.

3.5 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA CUALIFICADA PARA REPRESENTANTES DE PERSONAS JURÍDICAS [CENTRALIZADO]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.3.25. Política ETSI: QCP-n-qscd (OID: 0.4.0.194112.1.2). OID del perfil del Ministerio de Hacienda y Administraciones Públicas: 2.16.724.1.3.5.8.

Estos certificados son certificados cualificados de firma electrónica de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo cualificado de creación de firma electrónica (QSCD), de acuerdo con el Anexo II del Reglamento (UE) 910/2014.

Estos certificados son gestionados de forma centralizada, es decir, la generación y gestión de los datos de creación de firma electrónica es realizada por el prestador, por cuenta del firmante.

Son certificados de representante de persona jurídica, con poderes totales, administrador único o solidario de la organización suscriptora del certificado, o al menos con poderes específicos generales para actuar ante terceros.

Estos certificados garantizan la identidad de la organización suscriptora del certificado y del firmante, indican una relación de representación legal o apoderamiento general entre el firmante y la organización suscriptora del certificado, y permiten la generación de la "firma electrónica cualificada", con efecto jurídico equivalente al de una firma manuscrita conforme al artículo 25.2 del Reglamento (UE) 910/2014.

Estos certificados incluyen un campo donde se indica el documento, público si resulta exigible, que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la persona jurídica a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales.

3.6 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA AVANZADA PARA REPRESENTANTES DE PERSONAS JURÍDICAS [SOFTWARE]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.3.21. Política ETSI: QCP-n (OID: 0.4.0.194112.1.0). OID del perfil del Ministerio de Hacienda y Administraciones Públicas: 2.16.724.1.3.5.8.

Estos certificados son certificados cualificados de firma electrónica de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados no funcionan con dispositivo cualificado de creación de firma electrónica (QSCD).

Estos certificados son gestionados de forma distribuida sin la participación de una herramienta de gestión centralizada.

Son certificados de representante de persona jurídica, con poderes totales, administrador único o solidario de la organización suscriptora del certificado, o al menos con poderes específicos generales para actuar ante terceros.

Estos certificados garantizan la identidad de la organización suscriptora del certificado y del firmante, indican una relación de representación legal o apoderamiento general entre el firmante y la organización suscriptora del certificado, y permiten la generación de la "firma electrónica avanzada" basada en certificado electrónico cualificado de firma electrónica.

Estos certificados incluyen un campo donde se indica el documento, público si resulta exigible, que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la persona jurídica a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales.

3.7 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA CUALIFICADA PARA REPRESENTANTES DE ENTIDADES SIN PERSONALIDAD JURÍDICA [CENTRALIZADO]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.3.35. Política ETSI: QCP-n-qscd (OID: 0.4.0.194112.1.2). OID del perfil del Ministerio de Hacienda y Administraciones Públicas: 2.16.724.1.3.5.9.

Estos certificados son certificados cualificados de firma electrónica de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo cualificado de creación de firma electrónica (QSCD), de acuerdo con el Anexo II del Reglamento (UE) 910/2014.

Estos certificados son gestionados de forma centralizada, es decir, la generación y gestión de los datos de creación de firma electrónica es realizada por el prestador, por cuenta del firmante.

Son certificados de representante de entidad sin personalidad jurídica, con poderes totales, administrador único o solidario de la organización suscriptora del certificado, o al menos con poderes específicos generales para actuar ante terceros.

Estos certificados garantizan la identidad de la organización suscriptora del certificado y del firmante, indican una relación de representación legal o apoderamiento general entre el firmante y la organización suscriptora del certificado, y permiten la generación de la "firma electrónica cualificada", con efecto jurídico equivalente al de una firma manuscrita conforme al artículo 25.2 del Reglamento (UE) 910/2014.

Estos certificados incluyen un campo donde se indica el documento, público si resulta exigible, que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la entidad sin personalidad jurídica a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales.

3.8 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA AVANZADA PARA REPRESENTANTES DE ENTIDADES SIN PERSONALIDAD JURÍDICA [SOFTWARE]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.3.31. Política ETSI: QCP-n (OID: 0.4.0.194112.1.0). OID del perfil del Ministerio de Hacienda y Administraciones Públicas: 2.16.724.1.3.5.9.

Estos certificados son certificados cualificados de firma electrónica de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados no funcionan con dispositivo cualificado de creación de firma electrónica (QSCD).

Estos certificados son gestionados de forma distribuida sin la participación de una herramienta de gestión centralizada.

Son certificados de representante de entidad sin personalidad jurídica, con poderes totales, administrador único o solidario de la organización suscriptora del certificado, o al menos con poderes específicos generales para actuar ante terceros.

Estos certificados permiten la generación de la "firma electrónica avanzada" basada en certificado electrónico cualificado.

Estos certificados garantizan la identidad de la organización suscriptora del certificado y del firmante, indican una relación de representación legal o apoderamiento general entre el firmante y la organización suscriptora del certificado, y permiten la generación de la "firma electrónica avanzada" basada en certificado electrónico cualificado de firma electrónica.

Estos certificados incluyen un campo donde se indica el documento, público si resulta exigible, que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la entidad sin personalidad jurídica a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales.

3.9 CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO CUALIFICADO PARA AAPP [CENTRALIZADO-NIVEL ALTO]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.2.15. Política ETSI: QCP-l-qscd (OID: 0.4.0.194112.1.3). OID del perfil del Ministerio de Hacienda y Administraciones Públicas: 2.16.724.1.3.5.6.1.

Estos certificados son certificados cualificados de sello electrónico de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo cualificado de creación de sello electrónico (QSCD), de acuerdo con el Anexo II del Reglamento (UE) 910/2014.

Estos certificados son gestionados de forma centralizada, es decir, la generación y gestión de los datos de creación de sello electrónico es realizada por el prestador, por cuenta del creador del sello.

Estos certificados garantizan la identidad del creador del sello (Administración Publica) y permiten la generación del “sello electrónico cualificado”, que disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos conforme al artículo 35.2 del Reglamento (UE) 910/2014.

3.10 CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO AVANZADO PARA AAPP [SOFTWARE-NIVEL MEDIO]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.2.11. Política ETSI: QCP-l (OID: 0.4.0.194112.1.1). OID del perfil del Ministerio de Hacienda y Administraciones Públicas: 2.16.724.1.3.5.6.2.

Estos certificados son certificados cualificados de sello electrónico de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados no funcionan con dispositivo cualificado de creación de sello electrónico (QSCD).

Estos certificados son gestionados de forma distribuida sin la participación de una herramienta de gestión centralizada.

Estos certificados garantizan la identidad del creador del sello (Administración Publica), y permiten la generación del “sello electrónico avanzado” basado en certificado cualificado de sello electrónico.

3.11 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA CUALIFICADA PARA EMPLEADOS PÚBLICOS [CENTRALIZADO-NIVEL ALTO]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.3.55. Política ETSI: QCP-n-qscd (OID: 0.4.0.194112.1.2). OID del perfil del Ministerio de Hacienda y Administraciones Públicas: 2.16.724.1.3.5.7.1.

Estos certificados son certificados cualificados de firma electrónica de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo cualificado de creación de firma electrónica (QSCD), de acuerdo con el Anexo II del Reglamento (UE) 910/2014.

Estos certificados son gestionados de forma centralizada, es decir, la generación y gestión de los datos de creación de firma electrónica es realizada por el prestador, por cuenta del firmante.

Estos certificados garantizan la identidad del firmante y su vinculación como empleado público con la organización suscriptora del certificado, y permiten la generación de la "firma electrónica cualificada", con efecto jurídico equivalente al de una firma manuscrita conforme al artículo 25.2 del Reglamento (UE) 910/2014.

3.12 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA AVANZADA PARA EMPLEADOS PÚBLICOS [SOFTWARE-NIVEL MEDIO]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.3.51. Política ETSI: QCP-n (OID: 0.4.0.194112.1.0). OID del perfil del Ministerio de Hacienda y Administraciones Públicas: 2.16.724.1.3.5.7.2.

Estos certificados son certificados cualificados de firma electrónica de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados no funcionan con dispositivo cualificado de creación de firma electrónica (QSCD).

Estos certificados son gestionados de forma distribuida sin la participación de una herramienta de gestión centralizada.

Estos certificados garantizan la identidad del firmante y su vinculación como empleado público con la organización suscriptora del certificado, y permiten la generación de la "firma electrónica avanzada" basada en certificado cualificado de firma electrónica.

3.13 CERTIFICADO CUALIFICADO DE FIRMA ELECTRÓNICA CUALIFICADA PARA EMPLEADOS PÚBLICOS CON SEUDÓNIMO [CENTRALIZADO-NIVEL ALTO]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.3.65. Política ETSI: QCP-n-qscd (OID: 0.4.0.194112.1.2). OID del perfil del Ministerio de Hacienda y Administraciones Públicas: 2.16.724.1.3.5.4.1.

Estos certificados son certificados cualificados de firma electrónica de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo cualificado de creación de firma electrónica (QSCD), de acuerdo con el Anexo II del Reglamento (UE) 910/2014.

Estos certificados son gestionados de forma centralizada, es decir, la generación y gestión de los datos de creación de firma electrónica es realizada por el prestador, por cuenta del firmante.

Estos certificados garantizan la identidad del firmante, por medio de un seudónimo, y su vinculación como empleado público con la organización suscriptora del certificado, y permiten la generación de la “firma electrónica cualificada”, con efecto jurídico equivalente al de una firma manuscrita conforme al artículo 25.2 del Reglamento (UE) 910/2014.

3.14 CERTIFICADO CUALIFICADOS DE FIRMA ELECTRÓNICA AVANZADA PARA EMPLEADOS PÚBLICOS CON SEUDÓNIMO [SOFTWARE-NIVEL MEDIO]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.3.61. Política ETSI: QCP-n (OID: 0.4.0.194112.1.0). OID del perfil del Ministerio de Hacienda y Administraciones Públicas: 2.16.724.1.3.5.4.2.

Estos certificados son certificados cualificados de firma electrónica de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados no funcionan con dispositivo cualificado de creación de firma electrónica (QSCD).

Estos certificados son gestionados de forma distribuida sin la participación de una herramienta de gestión centralizada.

Estos certificados garantizan la identidad del firmante, por medio de un seudónimo, y su vinculación como empleado público con la organización suscriptora del certificado, y permiten la generación de la “firma electrónica avanzada” basada en certificado cualificado de firma electrónica.

3.15 CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO CUALIFICADO PARA PERSONA JURÍDICAS [CENTRALIZADO]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.2.5. Política ETSI: QCP-l-qscd (OID: 0.4.0.194112.1.3).

Estos certificados son certificados cualificados de sello electrónico de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo cualificado de creación de sello electrónico (QSCD), de acuerdo con el Anexo II del Reglamento (UE) 910/2014.

Estos certificados son gestionados de forma centralizada, es decir, la generación y gestión de los datos de creación de sello electrónico es realizada por el prestador, por cuenta del creador del sello.

Estos certificados garantizan la identidad del creador del sello y permiten la generación del "sello electrónico cualificado", que disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos conforme al artículo 35.2 del Reglamento (UE) 910/2014.

3.16 CERTIFICADO CUALIFICADO DE SELLO ELECTRÓNICO AVANZADO PARA PERSONAS JURÍDICAS [SOFTWARE]

OID de DIGITEL TS: 1.3.6.1.4.1.54225.10.2.1. Política ETSI: QCP-l (OID: 0.4.0.194112.1.1).

Estos certificados son certificados cualificados de sello electrónico de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 y dan cumplimiento a lo dispuesto por la normativa técnica ETSI EN 319 411-2.

Estos certificados no funcionan con dispositivo cualificado de creación de sello electrónico (QSCD).

Estos certificados son gestionados de forma distribuida sin la participación de una herramienta de gestión centralizada.

Estos certificados garantizan la identidad del creador del sello, y permiten la generación del "sello electrónico avanzado" basado en certificado cualificado de sello electrónico.

4. PERIODO DE VALIDEZ DE LOS CERTIFICADOS

El periodo de validez será el que se indique en el propio certificado. No obstante, DIGITEL TS emite todos los tipos de certificados cualificados de firma electrónica y sello electrónico con validez de 3 años, 2 años y 48 horas.

5. LÍMITES DE USO Y LÍMITES DE CONFIANZA DE LOS CERTIFICADOS

5.1 LÍMITES DE USO DIRIGIDOS A LOS FIRMANTES Y CREADORES DE SELLOS

El firmante o el creador de sello ha de utilizar el servicio de emisión de certificados cualificados prestado por DIGITEL TS exclusivamente para los usos autorizados en el contrato firmado entre DIGITEL TS y el suscriptor, y que se reproducen posteriormente (sección "obligaciones de los firmantes y creadores de sellos"). Asimismo, el firmante o el creador del sello se obliga a utilizar el servicio cualificado de emisión de certificados cualificados de acuerdo con las instrucciones, manuales o procedimientos suministrados por DIGITEL TS.

El firmante o el creador del sello ha de cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas que emplee.

El firmante o el creador del sello no puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de emisión de certificados cualificados de DIGITEL TS, sin previo permiso expreso.

Los certificados emitidos conforme a las políticas QCP-n-qscd y QCP-l-qscd requieren el uso de un dispositivo cualificado de creación de firma o sello electrónico (QSCD). En los certificados centralizados, dicho dispositivo es gestionado por DIGITEL TS por cuenta del firmante o del creador del sello.

5.2 LÍMITES DE USO DIRIGIDOS A LOS VERIFICADORES

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Excepto cuando se prevea expresamente en un procedimiento de la Autoridad de Certificación de DIGITEL TS, los certificados no pueden emplearse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (CRL), sin perjuicio de lo indicado en el artículo 24.1 bis letra b) del Reglamento (UE) 910/2014 .

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites de uso indicados en los campos y las extensiones de los perfiles de certificados, los cuales no incluyen la función de cifrado de claves ni de otros tipos de datos. En todo caso, DIGITEL TS no responderá por pérdida alguna de información cifrada con la clave pública contenida en los certificados emitidos que no se pueda recuperar por la pérdida de la clave privada o del acceso a la misma por el titular del certificado necesario para descifrar la información.

El empleo de los certificados en operaciones que contravienen este declaración de divulgación, la declaración de prácticas o los contratos con los suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a DIGITEL TS, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

DIGITEL TS no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de DIGITEL TS emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor o la persona responsable del uso de los datos de creación de firma o sello electrónico del certificado cualquier responsabilidad derivada del contenido aparejado al uso de los mismos. Todo ello sin perjuicio del régimen aplicable a los servicios de la sociedad de la información, cuando sea legalmente procedente.

Asimismo, le será imputable al suscriptor o a la persona responsable del uso de los datos de creación de firma o sello electrónico del certificado cualquier responsabilidad que pudiese derivarse de la utilización de los mismos fuera de los límites y condiciones de uso recogidas en esta declaración de divulgación, o en los contratos con los suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

5.3 LÍMITES DE CONFIANZA (RELIANCE LIMITS)

Los certificados cualificados emitidos por DIGITEL TS están destinados para su uso con firmas electrónicas o sellos electrónicos, según corresponda al tipo de certificado, además de para realizar autenticaciones de cliente en el acceso a servicios web o TLS.

6. OBLIGACIONES DE LOS SUSCRIPTORES

Las obligaciones del suscriptor, conforme a lo previsto en la cláusula 6.3.5 (OVR-6.3.5-01 y OVR-6.3.5-02) de la norma ETSI EN 319 411-1, incluyen las siguientes:

6.1 GENERACIÓN DE CLAVES

El suscriptor autoriza a DIGITEL TS a generar las claves, privada y pública, para la identificación y la firma electrónica de los firmantes, y solicita en su nombre la emisión del certificado, y/o para la identificación y el sello electrónico del creador del sello.

6.2 SOLICITUD DE CERTIFICADOS

El suscriptor se obliga a realizar las solicitudes de los certificados de acuerdo con el procedimiento y, si es necesario, los componentes técnicos suministrados por DIGITEL TS, de conformidad con lo que se establece en la declaración de prácticas y políticas de certificación (DPPC) y en la documentación de operaciones de DIGITEL TS.

6.3 OBLIGACIONES DE INFORMACIÓN

El suscriptor se responsabiliza de que toda la información incluida en su solicitud del certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.

El suscriptor tiene que informar inmediatamente a DIGITEL TS:

- De cualquier inexactitud detectada en el certificado una vez se haya emitido.
- De los cambios que se produzcan en la información aportada y/o registrada para la emisión del certificado.
- De la pérdida, robo, sustracción, o cualquier otro tipo de pérdida de control de la clave privada por el firmante o el creador del sello.

6.4 OBLIGACIONES DE CUSTODIA

En su caso, el suscriptor se obliga a custodiar toda la información que genere en su actividad como Autoridad de Registro.

6.5 OBLIGACIONES ADICIONALES DEL SUSCRIPTOR

De conformidad con la cláusula 6.3.5 (OVR-6.3.5-01 y OVR-6.3.5-02) de la norma ETSI EN 319 411-1, las obligaciones adicionales del suscriptor incluyen:

a) Obligación de que el par de claves sea utilizado exclusivamente conforme a las limitaciones notificadas al suscriptor y al firmante o creador del sello.
b) Prohibición del uso no autorizado de la clave privada del firmante o creador de sellos.
c) Obligación de notificar sin demora a DIGITEL TS o a la Autoridad de Registro a través de la cual se emitió el certificado si la clave privada ha sido comprometida, si se ha perdido el control sobre los datos de activación, o si se detectan inexactitudes en el contenido del certificado.
d) Obligación de cesar inmediata y permanentemente en el uso de la clave privada tras su compromiso.
e) Obligación de cesar en el uso de la clave privada cuando el certificado haya sido revocado o cuando la Autoridad de Certificación emisora haya sido comprometida.

7. OBLIGACIONES DE LOS FIRMANTES Y CREADORES DE SELLOS

7.1 OBLIGACIONES DE CUSTODIA

El firmante y el creador del sello se obligan a custodiar el código de identificación personal o cualquier soporte técnico entregado por DIGITEL TS, las claves privadas y, si fuese necesario, las especificaciones propiedad de DIGITEL TS que le sean suministradas.

El firmante y el creador del sello se obligan a custodiar el código de identificación personal (PIN).

En caso de pérdida o robo de la clave privada del certificado, o en caso de que el firmante o el creador del sello sospeche que la clave privada ha perdido fiabilidad por cualquier motivo, dichas circunstancias han de ser notificadas inmediatamente a DIGITEL TS o a la Autoridad de Registro a través de la cual se emitió el certificado, directamente o por medio del suscriptor.

7.2 OBLIGACIONES DE USO CORRECTO

El firmante y el creador del sello tienen que utilizar el servicio de emisión de certificados cualificados prestado por DIGITEL TS, exclusivamente para los usos autorizados en la DPPC y en cualquier otra instrucción, manual o procedimiento suministrado al suscriptor.

El firmante y el creador del sello tienen que cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas empleadas.

El firmante y el creador del sello no podrán adoptar medidas de inspección, alteración o descompilación de los servicios de certificación digital prestados.

El firmante y el creador del sello reconocerán:

a) Que cuando utilice cualquier certificado, y mientras el certificado no haya expirado ni haya sido suspendido o haya sido revocado, habrá aceptado dicho certificado y estará operativo.
b) Que no actúa como Autoridad de Certificación y, por lo tanto, se obliga a no utilizar las claves privadas correspondientes a las claves públicas contenidas en los certificados con el propósito de firmar certificado alguno.
c) Que en caso de quedar comprometida la clave privada, su uso queda inmediata y permanentemente suspendido.
d) En los certificados emitidos conforme a las políticas QCP-n-qscd y QCP-l-qscd, el firmante o el creador del sello se obligan a utilizar la clave privada exclusivamente dentro del dispositivo cualificado de creación de firma o sello (QSCD).

7.3 TRANSACCIONES PROHIBIDAS

El firmante y el creador del sello se obligan a no utilizar sus claves privadas, los certificados o cualquier otro soporte técnico entregado por DIGITEL TS en la realización de transacción alguna prohibida por la ley aplicable.

Los servicios de emisión de certificados cualificados prestados por DIGITEL TS no han sido diseñados ni permiten su utilización o reventa como equipos de control de situaciones peligrosas, o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo o sistemas de control de armamento, en las que un error pudiera directamente causar la muerte, daños físicos o daños medioambientales graves.

8. OBLIGACIONES DE LOS VERIFICADORES

Conforme a lo previsto en la cláusula 6.3.5 (OVR-6.3.5-03) de la norma ETSI EN 319 411-1, las obligaciones de las partes que confían en los certificados son las siguientes:

8.1 DECISIÓN INFORMADA

DIGITEL TS informa al verificador que tiene acceso a información suficiente para tomar una decisión informada en el momento de verificar un certificado y confiar en la información contenida en dicho certificado.

Adicionalmente, el verificador reconocerá que el uso de las Listas de Revocación de Certificados (en lo sucesivo, las CRL) y del servicio OCSP de DIGITEL TS, se rigen por la DPPC de DIGITEL TS y se comprometerá a cumplir los requisitos técnicos, operativos y de seguridad descritos en la mencionada DPPC.

8.2 REQUISITOS DE VERIFICACIÓN DE LA FIRMA DIGITAL

La comprobación será ejecutada normalmente de forma automática por el software del verificador y, en todo caso, de acuerdo con la DPPC, con los siguientes requisitos:

- Es necesario utilizar el software apropiado para la verificación de una firma digital (firma electrónica o sello electrónico) con los algoritmos y longitudes de claves autorizados en el certificado y/o ejecutar cualquier otra operación criptográfica, y establecer la cadena de certificados en que se basa la firma digital a verificar, ya que la firma digital se verifica utilizando esta cadena de certificados.
    - Es necesario asegurar que la cadena de certificados identificada es la más adecuada para la firma digital que se verifica, ya que una firma digital puede basarse en más de una cadena de certificados, y es decisión del verificador asegurarse el uso de la cadena más adecuada para verificarla.
    - Es necesario comprobar el estado de revocación de los certificados de la cadena con la información suministrada por DIGITEL TS (CRL o servicio OCSP) para determinar la validez de todos los certificados de la cadena de certificados, ya que únicamente puede considerarse correctamente verificada una firma electrónica si todos y cada uno de los certificados de la cadena son correctos y se encuentran vigentes.

- Es necesario asegurar que todos los certificados de la cadena autorizan el uso de la clave privada por el firmante o el creador del sello, ya que existe la posibilidad de que alguno de los certificados incluya límites de uso que impidan confiar en la firma digital que se verifica. Cada certificado de la cadena dispone de un indicador que hace referencia a las condiciones de uso aplicables, para su revisión por los verificadores.

- Es necesario verificar técnicamente la firma digital de todos los certificados de la cadena antes de confiar en el certificado utilizado por el firmante.

8.3 CONFIANZA EN UN CERTIFICADO NO VERIFICADO

Si el verificador confía en un certificado no verificado, asumirá todos los riesgos derivados de esta actuación.

8.4 EFECTO DE LA VERIFICACIÓN

En virtud de la correcta verificación de los certificados, de conformidad con esta declaración de divulgación, el verificador puede confiar en la identificación y, en su caso, la clave pública del firmante o del creador del sello, dentro de las limitaciones de uso correspondientes

8.5 USO CORRECTO Y ACTIVIDADES PROHIBIDAS

El verificador se obliga a no utilizar ningún tipo de información de estado de los certificados o de ningún otro tipo que haya sido suministrada por DIGITEL TS, en la realización de transacción alguna prohibida para la ley aplicable a la citada transacción.

El verificador se obliga a no inspeccionar, interferir o realizar ingeniería inversa de la implantación técnica de los servicios públicos de certificación de DIGITEL TS, sin previo consentimiento escrito.

Adicionalmente, el verificador se obliga a no comprometer intencionadamente la seguridad de los servicios públicos de emisión de certificados cualificados de DIGITEL TS.

Los servicios de emisión de certificados cualidicados prestados por DIGITEL TS no han sido diseñados ni permiten la utilización o reventa, como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armamento, donde un error podría causar la muerte, daños físicos o daños medioambientales graves.

8.6 CLÁUSULA DE INDEMNIDAD

El tercero que confía en el certificado se compromete a mantener indemne a DIGITEL TS de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.
- Falta de comprobación de la totalidad de medidas de aseguramiento prescritas en la DPPC o resto de normas de aplicación.

DIGITEL TS no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar. DIGITEL TS no será responsable de los daños y perjuicios ocasionados en los términos indicados en el artículo 11 de Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

9. OBLIGACIONES DE DIGITEL TS

En relación con la prestación de los servicios de emisión de certificados cualificados, DIGITEL TS se obliga a:

- Emitir, entregar, administrar, suspender, revocar y renovar certificados, de acuerdo con las instrucciones suministradas por el suscriptor, en los casos y por los motivos descritos en la DPPC de DIGITEL TS.
- Ejecutar los servicios con los medios técnicos y materiales adecuados, y con personal que cumpla las condiciones de cualificación y experiencia establecidas en la DPPC.
- Cumplir los niveles de calidad del servicio, en conformidad con lo que se establece en la DPPC, en los aspectos técnicos, operativos y de seguridad.
- Notificar al suscriptor, con anterioridad a la fecha de expiración de los certificados, de la posibilidad de renovarlos.
- Notificar a los firmantes y creadores de sellos la revocación de los certificados, cuando se produzca dicha circunstancia.
- Comunicar a las terceras personas que lo soliciten, el estado de los certificados, de acuerdo con lo que se establece en la DPPC para los diferentes servicios de verificación de certificados.

En relación con las comprobaciones del registro

DIGITEL TS se obliga a la emisión de certificados en base a los datos suministrados por el suscriptor, por lo cual podrá realizar las comprobaciones que considere oportunas respecto de la identidad y otras informaciones personales y complementarias de los suscriptores y, cuando resulte procedente, de los firmantes.

Estas comprobaciones podrán incluir la justificación documental aportada por el firmante por medio del suscriptor, si DIGITEL TS lo considera necesario, y cualquier otro documento e información relevantes facilitados por el suscriptor y/o el firmante.

En el caso que DIGITEL TS detecte errores en los datos que se deben incluir en los certificados o que justifican estos datos, podrá realizar los cambios que considere necesarios antes de emitir el

certificado o suspender el proceso de emisión y gestionar con el suscriptor la incidencia correspondiente. En caso de que DIGITEL TS corrija los datos sin gestión previa de la incidencia correspondiente con el suscriptor, deberá notificar los datos finalmente certificados al suscriptor.

DIGITEL TS se reserva el derecho a no emitir el certificado, cuando considere que la justificación documental resulte insuficiente para la correcta identificación y autenticación del suscriptor y/o del firmante.

Las anteriores obligaciones quedarán en suspenso en los casos en que el suscriptor actúe como Autoridad de Registro y disponga de los elementos técnicos correspondientes a la generación de claves, emisión de certificados y grabación de dispositivos de firma corporativos.

9.1 PERIODOS DE CONSERVACIÓN

DIGITEL TS conserva la información relativa a los servicios prestados de acuerdo con el artículo 24.2.h) del Reglamento (UE) 910/2014 , y el artículo 9.3 letra a) de la Ley 6/2020, durante al menos 15 años desde la expiración del certificado o la finalización del servicio prestado.

DIGITEL TS almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada.

10. GARANTÍAS LIMITADAS Y RECHAZO DE GARANTÍAS

Garantía de DIGITEL TS por los servicios de certificación digital

DIGITEL TS garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Autoridad de Certificación.
    - Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la DPPC.
- Que los servicios de revocación cumplen con todos los requisitos materiales establecidos en la DPPC.

DIGITEL TS garantiza al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- Que el certificado ha sido emitido al suscriptor y firmante identificado en el mismo y que el certificado ha sido aceptado.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la DPPC.

- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y depósito.

Adicionalmente, DIGITEL TS garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado cualificado, de acuerdo con el Anexo I (certificados de firma) o el Anexo III (certificados de sello) del Reglamento (UE) N.º 910/2014, modificado por el Reglamento (UE) N.º 2024/1183.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, de la persona física identificada en el certificado (firmante), se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Autoridad de Certificación, con los límites que se establezcan. En ningún caso DIGITEL TS responderá por caso fortuito y en caso de fuerza mayor.

10.1 EXCLUSIÓN DE LA GARANTÍA

DIGITEL TS rechaza toda otra garantía diferente a la anterior que no sea legalmente exigible. Específicamente, DIGITEL TS no garantiza software alguno utilizado por cualquier persona para firmar, verificar firmas, cifrar, descifrar, o utilizar de otra forma certificado digital alguno emitido por DIGITEL TS, excepto en los casos en que exista una declaración escrita en sentido contrario.

10.2 LIMITACIONES DE RESPONSABILIDAD

DIGITEL TS será responsable del daño causado ante el suscriptor y/o firmante o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, conforme a lo dispuesto en el artículo 13 del Reglamento (UE) 910/2014 y en el artículo 11 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. La cantidad máxima por la que DIGITEL TS responderá en el supuesto de actuación negligente en el cumplimiento de las obligaciones asumidas será de seis mil euros (6.000 €) por certificado.

10.3 COBERTURA DE SEGURO

DIGITEL TS dispone de una garantía de cobertura de responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el artículo 24.2.c) del Reglamento (UE) 910/2014 y con el artículo 9.3.b) de la Ley 6/2020, con un mínimo asegurado de 3.000.000 de euros.

11. ACUERDOS APLICABLES, DPPC Y POLÍTICA DE CERTIFICACIÓN

11.1 ACUERDOS APLICABLES

Los acuerdos aplicables al servicio de emisión de certificados cualificados de Digitel TS son los siguientes:

- Contrato del servicio de emisión de certificados cualificados, que regula la relación entre la Autoridad de Certificación de DIGITEL TS y el Solicitante/Suscriptor del certificado.
- Condiciones generales del servicio incorporadas en esta declaración de divulgación (PDS) y en la Declaración de Prácticas y Políticas de Certificación (DPPC).

11.2 DPPC

Los servicios de emisión de certificados cualificados de la Autoridad de Certificación de DIGITEL TS se regulan técnica y operativamente por la DPPC de la Autoridad de Certificación de DIGITEL TS, por sus actualizaciones posteriores, así como por documentación complementaria.

La DPPC y la documentación de operaciones se modifica periódicamente y se puede consultar en la página de Internet: https://pki.digitelts.es

12. POLÍTICA DE PRIVACIDAD

DIGITEL TS dispone de una política de privacidad en la DPPC, y regulación específica de la privacidad en relación con el proceso de registro, la confidencialidad del registro, la protección del acceso a la información personal, y el consentimiento del usuario, conforme a lo exigido por el Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

La información a que se refiere el apartado de períodos de conservación se conserva por los períodos indicados debidamente registrada y con garantías de seguridad e integridad.

En particular, la información de registro se conserva durante al menos 15 años desde la extinción del certificado o la finalización del servicio prestado. Las siguientes informaciones son mantenidas confidenciales: solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados; claves privadas generadas y/o almacenadas por el prestador de servicios de certificación; y registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.

13. POLÍTICA DE REINTEGRO

DIGITEL TS no reintegrará el coste del servicio de certificación en ningún caso.

14. LEY APLICABLE, RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

Las relaciones con la Autoridad de Certificación de DIGITEL TS se regirán por la ley española en materia de servicios de confianza vigente en cada momento, así como por la legislación civil y mercantil en lo que sea de aplicación.

La jurisdicción competente es la que se indica en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

En caso de discrepancia entre las partes, las partes intentarán la previa resolución amistosa. A tal fin, las partes deberán dirigir una comunicación a la Autoridad de Certificación de DIGITEL TS por cualquier medio que deje constancia a la dirección de contacto indicada en el punto 1 de este documento.

Si las partes no alcanzasen un acuerdo al respecto, cualquiera de ellas podrá someter el conflicto a la jurisdicción civil, con sujeción a los Tribunales del domicilio social de la Autoridad de Certificación de DIGITEL TS.

DIGITEL TS establece, en el contrato de suscriptor y en el presente PDS, los procedimientos de mediación y resolución de conflictos aplicables, conforme la norma ETSI EN 319 411-1.

15. ACREDITACIONES, SELLOS DE CALIDAD Y AUDITORÍAS DE CONFORMIDAD

La Autoridad de Certificación de DIGITEL TS se encuentra incluida en la lista de prestadores de confianza (TSL) española https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx

DIGITEL TS es una empresa comprometida con la seguridad y la calidad de sus servicios mediante la obtención y mantenimiento de la certificación ISO/IEC 27001:2022.

De acuerdo con lo indicado en el Reglamento (UE) 910/2014, la Autoridad de Certificación de DIGITEL TS realizará auditorías de conformidad cada 2 años y de seguimiento en los años intermedios. En el marco de dichas auditorías, DIGITEL TS verifica el cumplimiento de los controles definidos en los Reglamentos de Ejecución del Reglamento eIDAS aplicables a los servicios de emisión de certificados cualificados,

Los certificados cualificados emitidos por DIGITEL TS se ajustan a las siguientes normas técnicas:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- ETSI TS119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev.